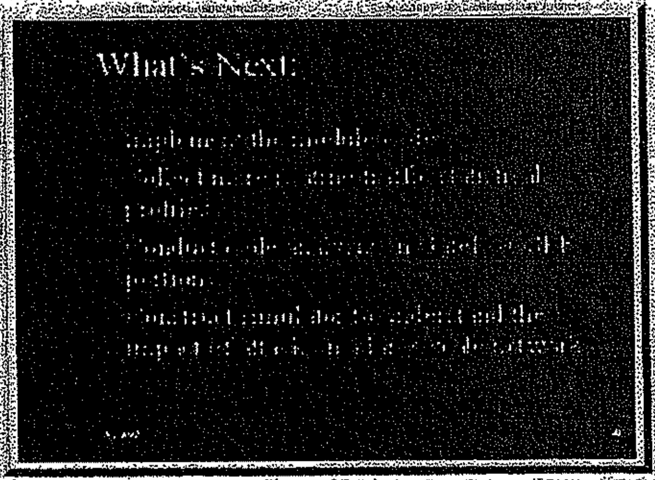


What's Next:

- Implement the modules [illegible]
- Collect more [illegible] statistical profiles
- Conduct [illegible] positions
- Construct [illegible] and the impact of [illegible]

Scalable Intrusion Detection for the Emerging Network Infrastructure

Scalable Intrusion Detection for the Emerging Network Infrastructure

Y. Frank Jou S. Felix Wu

MCNC NCSU

IDS Program Review

Next slide Back to the first slide View Graphic Version

Project Update

Project Update

- Overview
- System Architecture Design
- Routing Testbed Configuration
- Routing Traffic Statistical Profiles
- Routing Attacks
- What's next ...

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Overview: Target Environment

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Overview: JiNao Architecture

- Integration of attack prevention (configurable firewall) and intrusion detection.
- Detect your neighbors.
- A RSMM (Remote Security Management Module) can coordinate a set of JiNao's to detect orchestrated attacks and isolate bad routers.

Previous slide Next slide Back to the first slide View Graphic Version

System Design: ♂ Block Diagram

System Design: ♂ Block Diagram

Prevention Module

Detection Module

Decision Module

RSMM

SNMPv3 Eng.

Security

Officer

Previous slide Next slide Back to the first slide View Graphic Version

System Design: Intercept. Mod.

System Design: Intercept. Mod.

- May be placed in multiple protocol layers
  - Device driver
  - IP/IPSEC
  - Higher-layer protocols
- May facilitate active intrusion detection
  - Catch-and-Trap (through RSMM)
- May timestamp the packet

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: Prevention Mod.

- Prevention Layer: Go or No-Go
  - Quick response
- Extraction Layer
  - PDU format conversion
  - Multiple interception points correlation
    - e.g. This SNMPng/v3 PDU is from /dev/eth1 and /dev/tunnel

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: Protocol Analysis

- Maintain a set of Finite-State Machines
  - One FSM for each identified intrusion
- Provide extensibility
  - Reconfigurable at Run-Time
    - Table-driven implementation of FSMs
    - With a generic driver routine
  - Use Concurrency Workbench (CWB) to produce the FSMs

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: Statistical Analysis

- Unknown vulnerability detection
  - Complementary to rule-based and protocol-based analysis
- Profile training
  - Comparing short-term vs. long-term behaviors
    - Weighted aging: Favor more recent observation
  - Experimenting with NIDES statistical algorithm

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: Decision Mod.

- Make decisions on intrusion based on input from Prev/Detec Modules and RSMM
- Provide information for the IAM (RSMM)
- Propagate global information to the Prev/Detec Modules
- Notify security officer of faults/intrusion

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Router A

Router B

Correlate Input to make informed decision

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: Info. Abst. Mod.

- Detection Info. aggregation/MIB-fication
    - Run-length coding for data reduction for repeated normal report or persistent fault
- Periodic checking and propagation of global information
- Scope of Impact representation
    - Topological info. on all the affected routers through graph representation (GrIDS?)

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: MIB

- Rule/FSM configuration and statistical parameter specification
- Local detection results
- Detection notifications
- Security control
- Log access

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

System Design: RSMM

- SNMPv3-based management applications
- Access JiNao MIBs and correlate detection results
- Example: active intrusion detection (Catch and Trap)

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Alice

Bob

Chris

RSMM

Active Intrusion Detection: Catch &

Trap

(1)

(2)

(3)

(4)

(5)

(6)

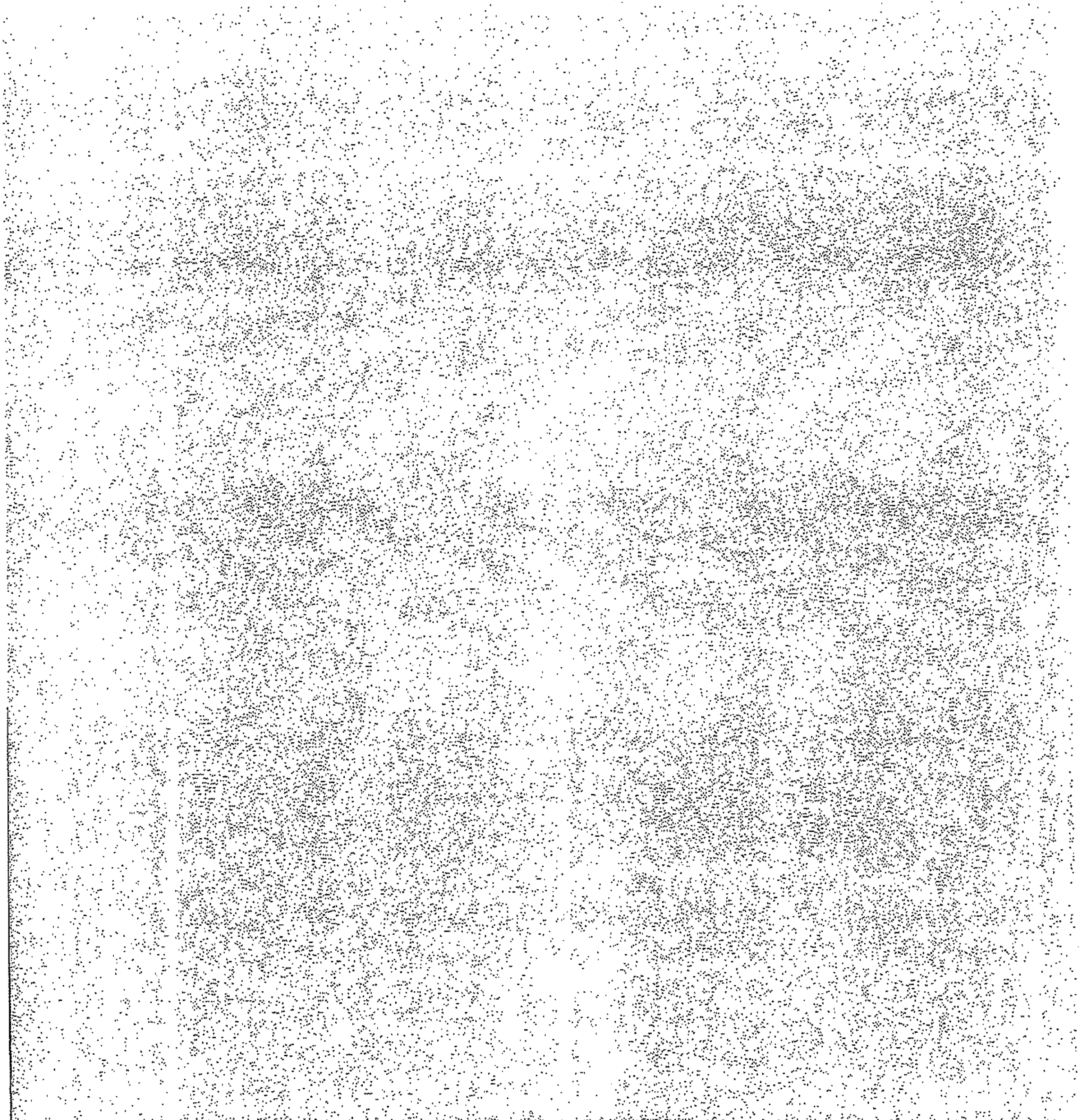
trap

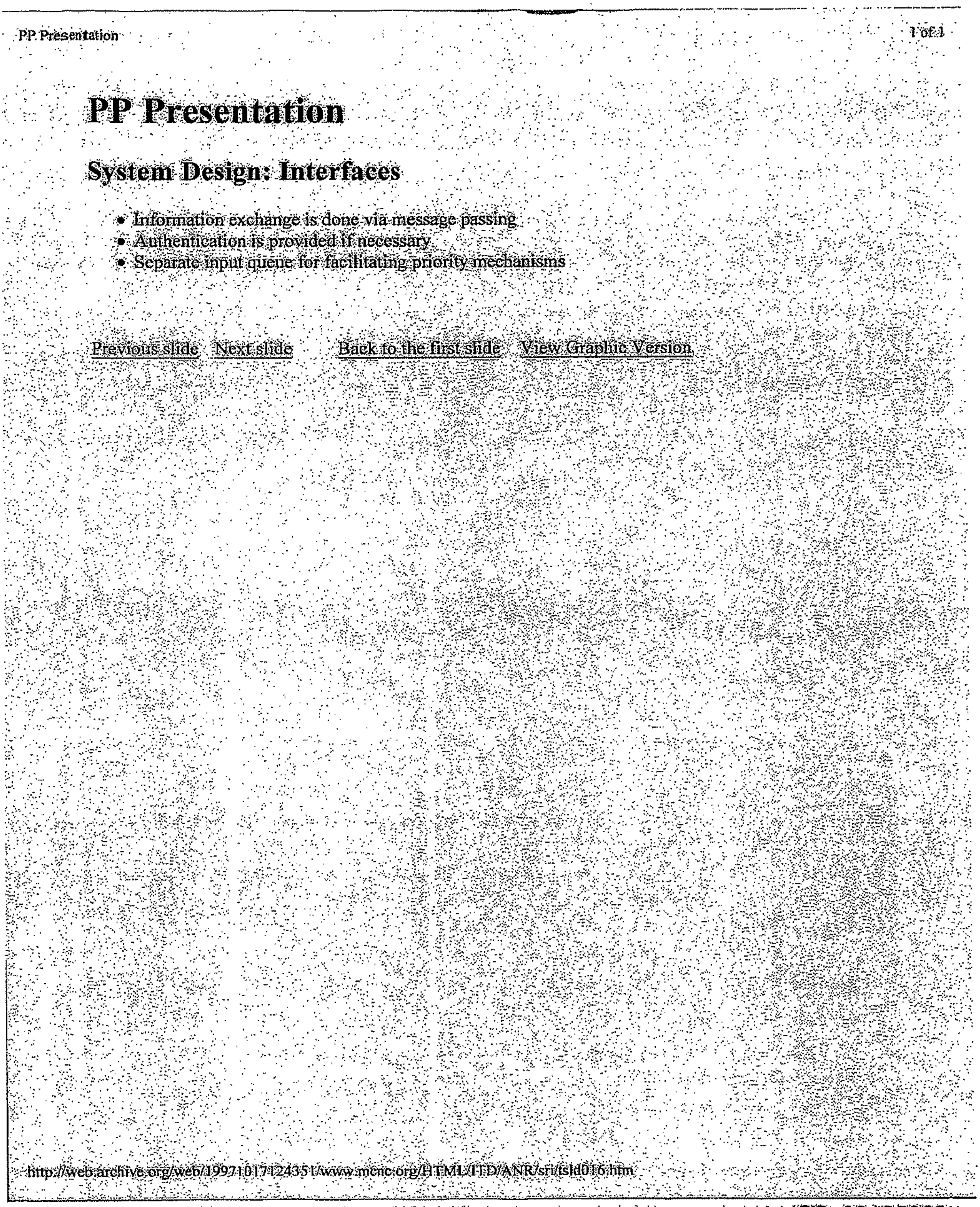
(7)

(0)

suspend

Previous slide Next slide Back to the first slide View Graphic Version





PP Presentation

System Design: Interfaces

- Information exchange is done via message passing
- Authentication is provided if necessary
- Separate input queue for facilitating priority mechanisms

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Testbed Configuration

- Two routing testbeds (autonomous systems, AS): MCNC & NCSU
- Each has three to four areas
- Allow independent code development
- Will be linked together to experiment ASBR attacks (only AS-external-LSAs are flooded throughout the entire AS)
- (Ref: configuration in file "testbed.ps")

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Routing Statistical Profiles

- Hello packets: stable (like step-function)
- Database Description and LS Request packets: rare events (only for forming adjacencies)
- LS Update and LS Ack: periodic in about every 30 min (LSRefreshTime: 30 min; MinLSInterval: 5 sec)
- (Look for four other postscript files, two were normal, two were under attack)

Previous slide Next slide Back to the first slide View Graphic Version